LISTING OF CLAIMS

1.   (Previously Presented) A method comprising:

associating a security association with a traffic stream;

associating a metric value with the security association;

modifying the metric value based on an amount of network traffic generated for the

traffic stream; and

dynamically mapping the traffic stream to one of multiple components that perform

cryptography operations based on the metric value.

2.   (Original) The method of claim 1 wherein the dynamic mapping is performed using a

time-based analysis.

3.   (Original) The method of claim 1 wherein the multiple components comprise a driver

agent and a network interface.

4.   (Original) The method of claim 1 wherein dynamically mapping traffic streams to one of

multiple components comprises selecting between performing cryptography operations with a

driver agent and performing cryptography operations with a network interface using cached

cryptography information.

5.   (Original) The method of claim 1 wherein the dynamic mapping further comprises

replacing a cached security association with a non-cached security association when the metric

value of the non-cached security association differs from the metric value of the cached security

association by at least a predetermined amount.

6.   (Original) The method of claim 5 wherein the predetermined amount is selected based on

a cost-based analysis.

Application No.: 09/895,344   Examiner: E.A. Shiferaw
Attorney Docket No.: 42390P11391   -2-   Art Unit: 2136

7.   (Original) The method of claim 1 wherein modifying the metric value further comprises initializing the metric to a predetermined value when the security association is received by a driver agent.

8.   (Original) The method of claim 1 wherein modifying the metric value further comprises changing the associated metric value by a predetermined amount when the security association is added to a cache.

9.   (Original) The method of claim 1 wherein modifying the metric value further comprises changing the associated metric value when a packet is received.

10.   (Original) The method of claim 1 wherein modifying the metric value further comprises periodically changing the metric value independent of network traffic.

11.   (Previously Presented) An apparatus comprising:

   a network interface coupled to receive network traffic streams; and

   a driver agent coupled to communicate with the network interface, the driver agent to associate a security association with a traffic stream, associate a metric value with the security association, modify the metric value of the security association based on how much network traffic is received for the traffic stream, and dynamically map the traffic stream to one of multiple components that perform cryptography operations based on the metric value.

12.   (Original) The apparatus of claim 11 wherein the dynamic mapping is performed using a time-based analysis.

13.   (Original) The apparatus of claim 11 wherein the multiple components comprise a driver agent and a network interface.

14.   (Original) The apparatus of claim 11 wherein dynamically mapping traffic streams to one of multiple components comprises selecting between performing cryptography operations with a

Application No.: 09/895,344   Examiner: B.A. Shiferaw
Attorney Docket No.: 42390P11391   -3-   Art Unit: 2136

PAGE 7/17 * RCVD AT 8/29/2005 7:23:40 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID:503 684 3245 * DURATION (mm-ss):06-04

driver agent and performing cryptography operations with a network interface using cached cryptography information.

15.   (Original) The apparatus of claim 11 wherein the dynamic mapping further comprises replacing a cached security association with a non-cached security association when the metric value of the non-cached security association is greater than the metric value of the cached security association by at least a predetermined amount.

16.   (Original) The apparatus of claim 15 wherein the predetermined amount is selected based on a cost-based analysis.

17.   (Original) The apparatus of claim 11 wherein modifying the metric value further comprises initializing the metric to a predetermined value when the security association is received by a driver agent.

18.   (Original) The apparatus of claim 11 wherein modifying the metric value further comprises changing the associated metric value by a predetermined amount when the security association is added to a cache.

19.   (Original) The apparatus of claim 11 wherein modifying the metric value further comprises changing the associated metric value when a packet is received.

20.   (Original) The apparatus of claim 11 wherein modifying the metric value further comprises periodically changing the metric value independent of network traffic.

21.   (Previously Presented) An article comprising a machine-accessible medium to provide machine-readable instructions that, when executed, cause one or more electronic systems to:

   associate a security association with a traffic stream;

   associate a metric value with the security association;

Application No.: 09/895,344   Examiner: E.A. Shiferaw
Attorney Docket No.: 42390P11391   -4-   Art Unit: 2136

PAGE 8/17 * RCVD AT 8/29/2005 7:23:40 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID:503 684 3245 * DURATION (mm-ss):06-04

modify the metric value based on an amount of network traffic generated for the traffic stream; and

dynamically map the traffic stream to one of multiple components that perform cryptography operations based on the metric value.

22.   (Original) The article of claim 21 wherein the dynamic mapping is performed using a time-based analysis.

23.   (Original) The article of claim 21 wherein the multiple components comprise a driver agent and a network interface.

24.   (Original) The article of claim 21 wherein dynamically mapping traffic streams to one of multiple components comprises selecting between performing cryptography operations with a driver agent and performing cryptography operations with a network interface using cached cryptography information.

25.   (Original) The article of claim 21 wherein the dynamic mapping further comprises replacing a cached security association with a non-cached security association when the metric value of the non-cached security association is greater than the metric value of the cached security association by at least a predetermined amount.

26.   (Original) The article of claim 25 wherein the predetermined amount is selected based on a cost-based analysis.

27.   (Original) The article of claim 21 wherein modifying the metric value further comprises initializing the metric to a predetermined value when the security association is received by a driver agent.

28.   (Original) The article of claim 21 wherein modifying the metric value further comprises changing the associated metric value by a predetermined amount when the security association is added to a cache.

29.   (Original) The article of claim 21 wherein modifying the metric value further comprises changing the associated metric value when a packet is received.

30.   (Original) The article of claim 21 wherein modifying the metric value further comprises periodically changing the metric value independent of network traffic.

31.   (Previously Presented) A electronic data signal embodied in a data communications medium shared among a plurality of network devices comprising sequences of instructions that, when executed, cause one or more electronic systems to:

associate a security association with a traffic stream;

associate a metric value with the security association;

modify the metric value based on an amount of network traffic generated for the traffic stream; and

dynamically map the traffic stream to one of multiple components that perform cryptography operations based on the metric value.

32.   (Original) The electronic data signal of claim 31 wherein the dynamic mapping is performed using a time-based analysis.

33.   (Original) The electronic data signal of claim 31 wherein the multiple components comprise a driver agent and a network interface.

34.   (Original) The electronic data signal of claim 31 wherein dynamically mapping traffic streams to one of multiple components comprises selecting between performing cryptography

Application No.: 09/895,344   Examiner: E.A. Shiferaw
Attorney Docket No.: 42390P11391   -6-   Art Unit: 2136

PAGE 10/17 * RCVD AT 8/29/2005 7:23:40 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID:503 684 3245 * DURATION (mm-ss):06-04

operations with a driver agent and performing cryptography operations with a network interface using cached cryptography information.

35.   (Original) The electronic data signal of claim 31 wherein the dynamic mapping further comprises replacing a cached security association with a non-cached security association when the metric value of the non-cached security association is greater than the metric value of the cached security association by at least a predetermined amount.

36.   (Original) The electronic data signal of claim 35 wherein the predetermined amount is selected based on a cost-based analysis.

37.   (Original) The electronic data signal of claim 31 wherein modifying the metric value further comprises initializing the metric to a predetermined value when the security association is received by a driver agent.

38.   (Original) The electronic data signal of claim 31 wherein modifying the metric value further comprises changing the associated metric value by a predetermined amount when the security association is added to a cache.

39.   (Original) The electronic data signal of claim 31 wherein modifying the metric value further comprises changing the associated metric value when a packet is received.

40.   (Original) The electronic data signal of claim 31 wherein modifying the metric value further comprises periodically changing the metric value independent of network traffic.

41.   (Previously Presented) A method comprising:

associating a security association with a traffic stream;

associating a metric value with a security association;

Application No.: 09/895,344   Examiner: E.A. Shiferaw
Attorney Docket No.: 42390P11391   -7-   Art Unit: 2136

PAGE 11/17 * RCVD AT 8/29/2005 7:23:40 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID:503 684 3245 * DURATION (mm-ss):06-04

initializing the metric value to a predetermined value when the security association is received by a driver agent, the metric value to be modified based at least in part on traffic generated for the associated traffic stream;

determining whether the security association necessary for performing cryptography operations on a packet of the traffic stream is cached;

determining whether the security association should be cached based on the metric value; and

caching the security association if it is determined from the metric value that the security association should be cached.

42.   (Canceled)

43.   (Previously Presented) The method of claim 41 wherein determining whether the security association should be cached further comprises:

increasing the value of the metric value by a predetermined amount when the associated security association is added to a cache;

incrementing the value of the metric value when a packet for the associated traffic stream is received; and

determining whether the metric value is greater than the lowest metric value of cached security associations by at least a predetermined amount.

44.   (Original) The method of claim 43 further comprising periodically decreasing the metric value.

45.   (Previously Presented) The method of claim 43 further comprising periodically evaluating the metric value to determine whether the security association should be cached.